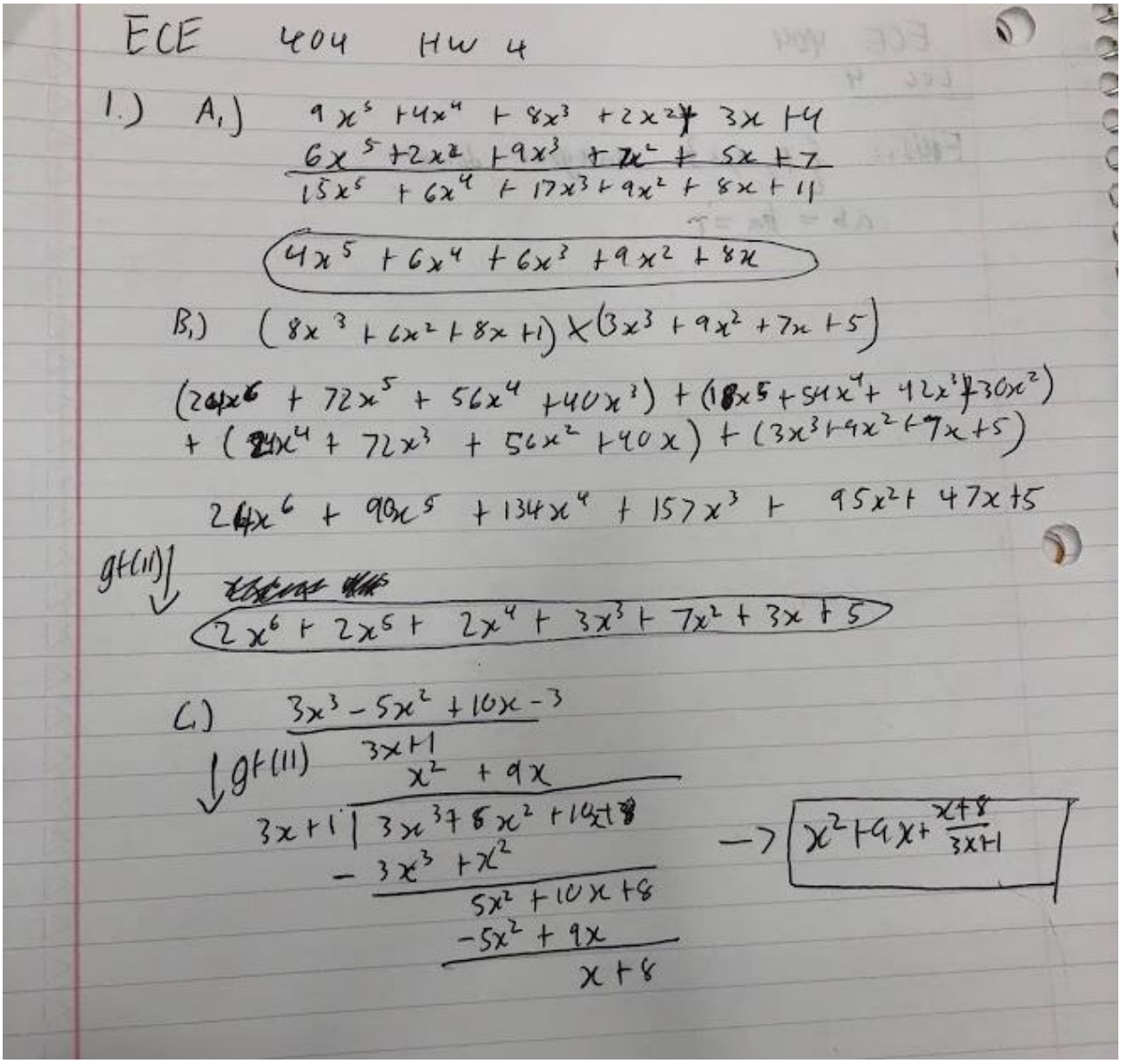
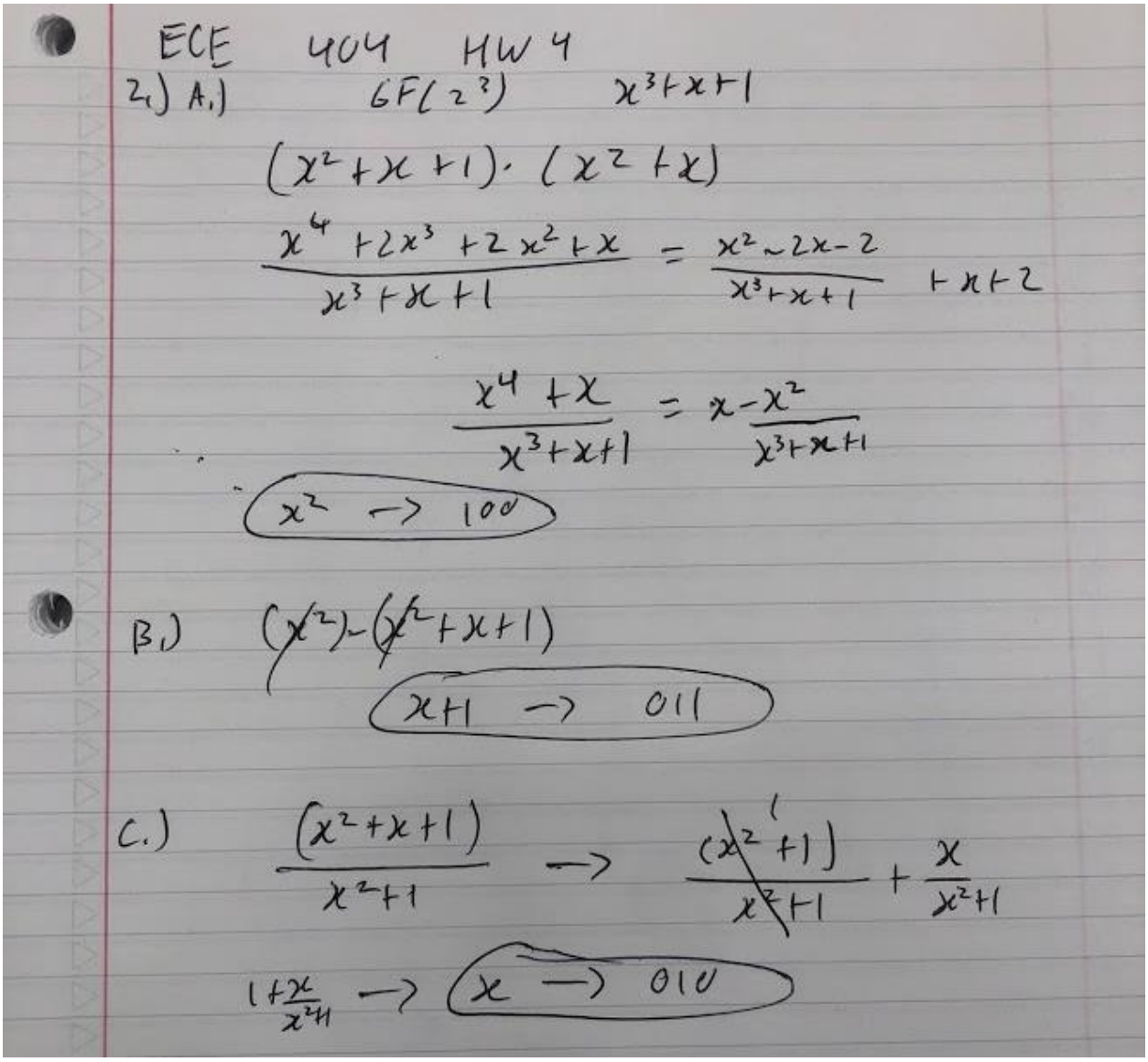
Theory Problems:

1:



2:


ECE 404 HW 4
2.) A.) GF(2^3) x^3+x+1
(x^2+x+1)·(x^2+x)
x^4+2x^3+2x^2+x / x^3+x+1 = x^2-2x-2 / x^3+x+1 + x+2
x^4+x / x^3+x+1 = x-x^2 / x^3+x+1
x^2 → 100
B.) (x^2)-(x^2+x+1)
x+1 → 011
C.) (x^2+x+1) / x^2+1 → (x^2+1) / x^2+1 + x / x^2+1
1+x / x^2+1 → x → 010

Programming Assignment:

In this we implement AES encryption utilizing its standard steps:

1. Byte substitution
2. Row Shifting
3. Mix Columns
4. Addition of the Round Keys

We create helper functions that we call in main to implement this process for encryptions